UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,398	01/16/2002	Germano Caronni	06502.0355	2081

7590 09/29/2005

Finnegan, Henderson, Farabow,
Garrett & Dunner, L.L.P.
1300 I Street, N.W.
Washington, DC 20005-3315

EXAMINER	
SMITHERS, MATTHEW	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/046,398	CARONNI ET AL.	
	Examiner	Art Unit	
	Matthew B. Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16,18-35 and 37-51* is/are rejected.

7)☒ Claim(s) *17 and 36* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/7/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

AT

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement filed October 7, 2003 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 8, 11, 21,29, 31,and 40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 8, 11, 21,29, 31,and 40 each recite the limitation "a first memory location" in the last line of the claims. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-16, 18-35, 37-51 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. patent 5,915,025 granted to Taguchi et al.

Regarding claim 1, Taguchi meets the claimed limitation as follows:

"A method for accessing information in a memory, comprising:

providing virtual address information to a memory management unit;

obtaining, from the memory management unit, a key tag and physical address information corresponding to the virtual address information;" see column 16, lines 44-59; column 17, lines 9-30 and Figure 17.

"retrieving a secret key using the key tag when it is determined that a memory location corresponding to the physical address information is protected; and

decrypting information read from the memory location using the secret key." see column 19, lines 16-37 and column 19, lines 54-59.

Regarding claim 2, Taguchi meets the claimed limitation as follows:

"The method of claim 1, the retrieving comprising:

looking up the secret key in a secret key table using the key tag based on a determination that the memory location is protected." see column 16, line 60 to column 17, line 8; column 20, lines 34-36 (. . . the selection . . . of a decryption key is dependent only on the target data to be protected.) and Figure 17.

Regarding claim 3, Taguchi meets the claimed limitation as follows:

"The method of claim 1, further comprising:

writing unencrypted data to the memory location based on a determination that the memory location is unprotected." see column 3, lines 27-40; column 11, lines 23-26;

and column 20, lines 34-36 (. . . the selection . . . of a decryption key is dependent only on the target data to be protected.).

Regarding claim 4, Taguchi meets the claimed limitation as follows:

"The method of claim 1, further comprising:

reading unencrypted data from the memory location based on a determination that the memory location is unprotected." see column 3, lines 27-40; column 11, lines 23-26; and column 20, lines 34-36 (. . . the selection . . . of a decryption key is dependent only on the target data to be protected.).

Regarding claim 5, Taguchi meets the claimed limitation as follows:

"The method of claim 1, further comprising:

executing an unencrypted instruction from the memory location based on a determination that the memory location is unprotected." see column 3, lines 27-40; column 11, lines 23-26; and column 20, lines 34-36 (. . . the selection . . . of a decryption key is dependent only on the target data to be protected.).

Regarding claim 6, Taguchi meets the claimed limitation as follows:

"The method of claim 1, wherein the decrypted information is an instruction, further comprising:

executing the instruction." see column 9, line 66 to column 10, line 31 (. . . causes decryption means to decrypt the encrypted data from the storage means . . . and executes instructions included in the data . . .) and column 21, line 57 to column 22, line 3 (. . . To execute instructions included in the data held in the storage means involves first having the data decrypted by the decryption means . . .).

Regarding claim 7, Taguchi meets the claimed limitation as follows:

"The method of claim 1, wherein the decrypted information is data." see column 9, line 66 to column 10, line 31 (. . . causes decryption means to decrypt the encrypted data from the storage means . . . and executes instructions included in the data . . .) and column 21, line 57 to column 22, line 3 (. . . To execute instructions included in the data held in the storage means involves first having the data decrypted by the decryption means . . .).

Regarding claim 8, Taguchi meets the claimed limitation as follows:

"The method of claim 1, further comprising:

encrypting data written to the first memory location using the secret key." see column 18, line 13 to column 19, line 15 and figure 19.

Regarding claim 9, Taguchi meets the claimed limitation as follows:

"A method for accessing information in a memory, comprising:

providing a virtual address to a memory management unit;

obtaining a key tag and a physical address corresponding to the virtual address from the memory management unit;

accessing a secret key in a secret key table using the key tag; and decrypting information read from a memory location corresponding to the physical address using the secret key." see column 16, lines 44-59; column 17, lines 9-30; column 19, lines 16-37 and column 19, lines 54-59 and Figure 17.

Regarding claim 10, Taguchi meets the claimed limitation as follows:

"A method for accessing information in a memory, comprising:

receiving a virtual address from a processor; retrieving a key tag and a physical address corresponding to the virtual address; and providing the key tag and the physical address to the processor, wherein a secret key associated with the key tag is used to decrypt information read from a memory location corresponding to the physical address." see column 8, lines 16-35 (Below . . .data processing apparatus . . . practiced as an embodiment of the invention . . .); column 16, lines 44-59; column 17, lines 9-30; column 19, lines 16-37 and column 19, lines 54-59 and Figure 17.

Regarding claim 11, Taguchi meets the claimed limitation as follows: "The method of claim 10, wherein the secret key is used to encrypt data written to the first memory location." see column 18, line 13 to column 19, line 15 and figure 19.

Regarding claim 12, Taguchi meets the claimed limitation as follows: "The method of claim 10, wherein the decrypted information is data." see column 9, line 66 to column 10, line 31 (. . . causes decryption means to decrypt the encrypted data from the storage means . . . and executes instructions included in the data . . .) and column 21, line 57 to column 22, line 3 (. . . To execute instructions included in the data held in the storage means involves first having the data decrypted by the decryption means . . .).

Regarding claim 13, Taguchi meets the claimed limitation as follows: "The method of claim 10, wherein the decrypted information is an instruction." see column 9, line 66 to column 10, line 31 (. . . causes decryption means to decrypt the encrypted data from the storage means . . . and executes instructions included in the data . . .) and column 21, line 57 to column 22, line 3 (. . . To execute instructions

included in the data held in the storage means involves first having the data decrypted by the decryption means . . .).

Regarding claim 14, Taguchi meets the claimed limitation as follows:

"The method of claim 10, the retrieving comprising:

looking up the key tag in a memory mapping table using the virtual address information." see column 16, line 60 to column 17, line 8; column 20, lines 34-36 (. . . the selection . . . of a decryption key is dependent only on the target data to be protected.) and Figure 17.

Regarding claim 15, Taguchi meets the claimed limitation as follows:

"A method for accessing information in a memory, comprising:

receiving, at a memory management unit, virtual address information from a processor;

retrieving a key tag and physical address information corresponding to the virtual address information;

sending, from the memory management unit to the processor, a key tag and physical address information corresponding to the virtual address information;

determining whether a memory location corresponding to the physical address information is protected based on the key tag; accessing a secret key in a secret key table using the key tag based on the determining; and decrypting information read from the memory location using the secret key." see column 8, lines 16-35 (Below . . .data processing apparatus . . . practiced as an embodiment of the invention . . .); column 16, lines 44-59; column 17, lines 9-30; column 19, lines 16-37 and column 19, lines 54-59 and Figure 17.

Regarding claim 16, Taguchi meets the claimed limitation as follows:

"A method for loading encrypted information into a memory, comprising:

determining whether a header associated with a program block includes an encrypted secret key;

decrypting the encrypted secret key to form a decrypted secret key when a result of the determination indicates that the header includes an encrypted secret key;

storing the decrypted secret key in a secret key table;

assigning the decrypted secret key a key tag for use in retrieving the decrypted secret key from the secret key table;

loading the program block into the memory at a first memory location; and

associating the key tag with virtual address information and physical address information corresponding to the memory location, wherein information read from the first memory location is decrypted using the decrypted secret key." see column 8, lines 16-35 (Below . . .data processing apparatus . . . practiced as an embodiment of the invention . . .); column 11, lines 26-45 (. . .key selection means includes a key determination means for determining the key corresponding to the data in each page . . . key determination means determines that the key group which corresponds to each block in the page. . . .); column 16, lines 44-59; column 17, lines 9-30; column 19, lines 16-37 and column 19, lines 54-59 and Figure 17.

Regarding claim 18, Taguchi meets the claimed limitation as follows:

"The method of claim 16, further comprising:

providing a key tag indicating that the program block is unencrypted based on a determination that the header does not include the encrypted secret key; loading the unencrypted program block into the memory at a second memory location; and associating the key tag indicating that the program block is unencrypted with virtual address information and physical address information corresponding to the second memory location." see column 8, lines 16-35 (Below . . .data processing apparatus . . . practiced as an embodiment of the invention . . .); column 11, lines 26-45 (. . .key selection means includes a key determination means for determining the key corresponding to the data in each page . . . key determination means determines that the key group which corresponds to each block in the page. . . .); column 16, lines 44-59; column 17, lines 9-30; column 19, lines 16-37 and column 19, lines 54-59 and Figure 17.

Regarding claim 19, Taguchi meets the claimed limitation as follows: "The method of claim 16, wherein the decrypted information is an instruction." see column 9, line 66 to column 10, line 31 (. . . causes decryption means to decrypt the encrypted data from the storage means . . . and executes instructions included in the data . . .) and column 21, line 57 to column 22, line 3 (. . . To execute instructions included in the data held in the storage means involves first having the data decrypted by the decryption means . . .).

Regarding claim 20, Taguchi meets the claimed limitation as follows: "The method of claim 16, wherein the decrypted information is data." see column 9, line 66 to column 10, line 31 (. . . causes decryption means to decrypt the encrypted data

from the storage means . . . and executes instructions included in the data . . .) and column 21, line 57 to column 22, line 3 (. . . To execute instructions included in the data held in the storage means involves first having the data decrypted by the decryption means . . .).

Regarding claim 21, Taguchi meets the claimed limitation as follows:
"The method of claim 16, wherein data written to the first memory location is encrypted using the decrypted secret key." see column 18, line 13 to column 19, line 15 and figure 19.

Claims 22, 23, 24, 25, 26, 27, 28 and 29 are apparatus claims that are substantially similar to method claims 1, 2, 3, 4, 5, 6, 7 and 8, respectively. Therefore, claims 22, 23, 24, 25, 26, 27, 28 and 29 are rejected by a similar rationale.
Claims 30, 31, 32, 33 and 34 are apparatus claims that are substantially similar to method claims 10, 11, 12, 13 and 14, respectively. Therefore, claims 30, 31, 32, 33, and 34 are rejected by a similar rationale.
Claims 35, 37, 38, 39 and 40 are apparatus claims that are substantially similar to method claims 16, 18, 19, 20 and 21, respectively. Therefore, claims 35, 37, 38, 39 and 40 are rejected by a similar rationale.

Regarding claim 41, Taguchi meets the claimed limitation as follows:
"A computer-readable medium containing instructions for performing a method for accessing information in a memory, the method comprising:

receiving, at a memory management unit, virtual address information from a processor;

retrieving a key tag and physical address information corresponding to the virtual address information;

sending, from the memory management unit to the processor, a key tag and physical address information corresponding to the virtual address information;

determining whether a memory location corresponding to the physical address information is protected based on the key tag; accessing a secret key in a secret key table using the key tag based on the determining;

and decrypting information read from the memory location using the secret key." see column 8, lines 16-35 (Below . . .data processing apparatus . . . practiced as an embodiment of the invention . . .); column 16, lines 44-59; column 17, lines 9-30; column 19, lines 16-37 and column 19, lines 54-59 and Figure 17.

Regarding claim 42, Taguchi meets the claimed limitation as follows:

"A computer-readable medium containing instructions for performing a method for loading encrypted information into a memory, the method comprising:

determining whether a header associated with a program block includes an encrypted secret key;

decrypting the encrypted secret key to form a decrypted secret key when a result of the determination indicates that the header includes an encrypted secret key;

storing the decrypted secret key in a secret key table;

assigning the decrypted secret key a key tag for use in retrieving the decrypted secret key from the secret key table;

loading the program block into the memory at a first memory location; and associating the key tag with virtual address information and physical address information corresponding to the memory location, wherein information read from the first memory location is decrypted using the decrypted secret key." see column 8, lines 16-35 (Below . . .data processing apparatus . . . practiced as an embodiment of the invention . . .); column 11, lines 26-45 (. . .key selection means includes a key determination means for determining the key corresponding to the data in each page . . . key determination means determines that the key group which corresponds to each block in the page. . . .); column 16, lines 44-59; column 17, lines 9-30; column 19, lines 16-37 and column 19, lines 54-59 and Figure 17.

Regarding claim 43, Taguchi meets the claimed limitation as follows:

"An apparatus for accessing information in a memory, comprising:

a processor; and

a memory management unit operable to receive a virtual address from the processor, retrieve a key tag and a physical address corresponding to the virtual address, and send the key tag and physical address to the processor, wherein the processor receives the key tag and physical address corresponding to the virtual address, determines whether a memory location corresponding to the physical address is protected based on the key tag, retrieves a secret key using the key tag based on the determining, and decrypts information read from the memory location using the secret key." see column 8, lines 16-35 (Below . . .data processing apparatus . . . practiced as an embodiment of the invention . . .); column 11, lines 26-45 (. . .key selection means includes a key

determination means for determining the key corresponding to the data in each page . . . key determination means determines that the key group which corresponds to each block in the page. . . .); column 16, lines 44-59; column 17, lines 9-30; column 19, lines 16-37 and column 19, lines 54-59 and Figure 17.

Regarding claim 44, Taguchi meets the claimed limitation as follows: "The apparatus of claim 43, wherein the processor writes unencrypted data to the memory location based on a determination that the first memory location is unprotected." see column 3, lines 27-40; column 11, lines 23-26; and column 20, lines 34-36 (. . . the selection . . . of a decryption key is dependent only on the target data to be protected.).

Regarding claim 45, Taguchi meets the claimed limitation as follows:

45. The apparatus of claim 43, wherein the processor reads unencrypted data from the memory location based on a determination that the first memory location is unprotected." see column 3, lines 27-40; column 11, lines 23-26; and column 20, lines 34-36 (. . . the selection . . . of a decryption key is dependent only on the target data to be protected.).

Regarding claim 46, Taguchi meets the claimed limitation as follows: "The apparatus of claim 43, wherein the processor executes an unencrypted instruction from the memory location based on a determination that the first memory location is unprotected." see column 3, lines 27-40; column 11, lines 23-26; and column 20, lines 34-36 (. . . the selection . . . of a decryption key is dependent only on the target data to be protected.).

Regarding claim 47, Taguchi meets the claimed limitation as follows: "The apparatus of claim 43, wherein the decrypted information is an instruction and the processor executes the instruction." see column 9, line 66 to column 10, line 31 (. . . causes decryption means to decrypt the encrypted data from the storage means . . . and executes instructions included in the data . . .) and column 21, line 57 to column 22, line 3 (. . . To execute instructions included in the data held in the storage means involves first having the data decrypted by the decryption means . . .).

Regarding claim 48, Taguchi meets the claimed limitation as follows: "The apparatus of claim 43, wherein the decrypted information is data." see column 9, line 66 to column 10, line 31 (. . . causes decryption means to decrypt the encrypted data from the storage means . . . and executes instructions included in the data . . .) and column 21, line 57 to column 22, line 3 (. . . To execute instructions included in the data held in the storage means involves first having the data decrypted by the decryption means . . .).

Regarding claim 49, Taguchi meets the claimed limitation as follows: "The apparatus of claim 43, wherein the processor encrypts data written to the memory location using the secret key." see column 18, line 13 to column 19, line 15 and figure 19.

Regarding claim 50, Taguchi meets the claimed limitation as follows: "An apparatus for loading encrypted information into a memory, comprising: a memory including a program that: determines whether a header associated with a program block includes an encrypted secret key; decrypts the encrypted secret key to

form a decrypted secret key when a result of the determination indicates that the header includes an encrypted secret key; stores the decrypted secret key in a secret key table; assigns the decrypted secret key a key tag for use in retrieving the decrypted secret key from the secret key table; loads the program block into the memory at a memory location; and associates the key tag with virtual address information and physical address information corresponding to the memory location, wherein information read from the memory location is decrypted using the decrypted secret key; and

a processor that runs the program." see column 8, lines 16-35 (Below . . .data processing apparatus . . . practiced as an embodiment of the invention . . .); column 11, lines 26-45 (. . .key selection means includes a key determination means for determining the key corresponding to the data in each page . . . key determination means determines that the key group which corresponds to each block in the page. . . .); column 16, lines 44-59; column 17, lines 9-30; column 19, lines 16-37 and column 19, lines 54-59 and Figure 17.

Regarding claim 51, Taguchi meets the claimed limitation as follows:

"A method for protecting information in a memory, comprising:

generating a secret key in response to instructions from a program;

storing the secret key in a secret key table;

assigning the secret key a key tag for use in retrieving the secret key from the secret key table; and

associating the key tag with virtual address information and physical address information corresponding to a memory location of a program block from the program,

wherein information read from the memory location is decrypted using the secret key." see column 8, lines 16-35 (Below . . .data processing apparatus . . . practiced as an embodiment of the invention . . .); column 11, lines 26-45 (. . .key selection means includes a key determination means for determining the key corresponding to the data in each page . . . key determination means determines that the key group which corresponds to each block in the page. . . .); column 16, lines 44-59; column 17, lines 9-30; column 19, lines 16-37 and column 19, lines 54-59 and Figure 17.

Allowable Subject Matter

Claims 17 and 36 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

With respect to claims 17 and 36, the cited prior art fails to specifically teach validating a signature on the decrypted secret key before storing the decrypted secret key in the secret key table.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. McCarty (US patent 5,666,411) discloses a system for protecting computer software using a crypto translation unit.

B. Buer (US patent 6,523,118) discloses a secure cache controller system for handling encrypted data.

C. Enslinger (US patent 6,910,094) discloses a secure memory manager unit that uses multiple cryptographic algorithms.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B Smithers
Primary Examiner
Art Unit 2137